Position Paper

Bitkom views on EDPB Guidelines 8/2020 on Targeting of Social Media Users

19/10/2020

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of Trust & Security
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Introduction and Overview

Bitkom welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft Guidelines on the targeting of social media users. We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice and reduce legal uncertainty.

We therefore appreciate that the EDPB published the draft Guidelines and is collecting feedback from stakeholders across Europe.

1. Summary

While we welcome that the EDPB is addressing the topic of Targeting and the Ad-Ecosystem, we think that the EDPB's Draft Guidelines on Targeting Social Media Users need clarification with regard to the different roles of the participants of the ecosystem (esp. controller-processor, joint controllership). Furthermore, the Guidelines present a rather one-sided view that personalized advertising and other forms of service personalization are harmful without acknowledging the benefits it provides to people and businesses. Their interpretation of the GDPR could upend established practices and change the nature of business relationships in the ads ecosystem, imposing significant and longstanding harm on the ad-supported Internet. We will go into more detail and make suggestions for a more balanced approach that also ensures compliance with the GDPR in the following paragraphs.

2. Scope

The Guideline´s scope should be amended and clarified. The Guidelines purport to cover the ´targeting of social media users´ and to clarify the roles and responsibilities as between social media providers and targeters. The reasoning and examples set forth in the Guidelines demonstrate, however, that their scope is likely to cover a broader set of advertising practices. Indeed, any company that plays a role – any role – in delivering targeted advertising or personalized online services to people should be interested in the impact of the Guidelines. The EDPB should be explicit about their potential to impact on a broad cross-section of the Internet.[1]

3. Balanced elaborations needed

The Guidelines should be more balanced and also cover elaborations, examples and arguments for ad-supported uses of services. We do recognize that targeting, the ad-supported internet and personalized ads need to be conducted in a healthy, privacy-friendly and transparent way that supports the user´s control over their data and protects their data adequately. The free use of services is fuelled by the ads-supported ecosystem and we suggest including the benefits for the users in the Guidelines as well. Users notably benefit from receiving more relevant content or ads. These also generate important benefits for advertisers and publishers, especially for smaller publishers who depend on the revenue from targeted ads, and content creators who can monetize their content online. Advantages for users should therefore be taken into account when balancing the interests of users in the context of Article 6 (1) (f) GDPR. It should also be noted that users also make an active contribution to targeting and personalization, at least when they (in an informed way) deliberately disclose and share personal data. This role of the users should also be included in the Guidelines. The current Draft fails to recognize the benefits of ad-supported Internet and the role of the user.

Although many policymakers in Europe have long been suspicious of the ad-funded business model, the fact remains that European companies remain committed to this model. Ad-funded business models have supported European companies for decades. This commitment — and the accompanying recognition that imposing tight restrictions on advertising could have real costs

[1] Please also refer to the Bitkom Comments on the EDPB Guidelines on the Concept of Controller and Processor with regard to these concepts and their impact on the ads-ecosystem.

for society and businesses — is among the reasons certain questions of GDPR implementation (such as the scope of Article 6 I b)[2] and ePrivacy Regulation have proven so controversial. The Guidelines should acknowledge the benefits of the ecosystem they seek to regulate and strike a balanced approach to regulation.

4. Impact on the ads-ecosystem

The Guidelines fail to recognize the negative impact they will have on the ads ecosystem. The Guidelines — particularly its sections around joint controllership — will require a whole host of new actions by publishers, ad tech providers, and advertisers. From new consent experiences to new right-to-object processes to significant terms updates, these Guidelines will create new implementation burdens for a large number of businesses. As is frequently the case, these new burdens will fall disproportionately on smaller businesses, already struggling to recover from the COVID pandemic and who often do not have the means to implement new requirements which are not included in the GDPR and, hence, have not been part of previous GDPR compliance efforts and are also often in a weaker bargaining position. The Guidelines should acknowledge their impact on businesses and should provide ample time for businesses to adjust their practices to come into compliance.

5. Legal bases for data processing

The Guidelines take an overly narrow view of the appropriate legal bases for ads data processing. The Guidelines categorically dismiss contractual necessity as an appropriate legal basis for processing personal data — of any kind — for ads.[3] They reach this conclusion despite the fact that just a year ago, they issued guidelines stating that assessing what contractual necessity *´involves a . . . fact-based assessment of the processing´* that asks, among other things, about the *´mutual perspectives and expectations of the parties to the contract.´*

While these Guidelines concluded that *´[a]s a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services,´* but did not foreclose the ability for contractual necessity, depending on the specifics of the service, to

[2] Please see on Art. 6 I b and its connection to the ePrivacy regulation the Bitkom Position Paper: https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Comments-on-EDPB-Guidelines-on-Article-61b-GDPR.
[3] Please see our detailed elaborations on the issue here: https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Comments-on-EDPB-Guidelines-on-Article-61b-GDPR.

serve as a legal basis for the processing of non-sensitive data categories to show targeted ads on a service.

That contractual necessity would not available for even limited targeted options which suggests that any business showing any kind of targeted ads may be required to provide a service with lower-performing contextual ads, in-app payment, or subscriptions.

Article 6(1)(b) GDPR provides a lawful basis for the processing of personal data to the extent that "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". This supports the freedom to conduct a business, which is guaranteed by Article 16 of the Charter. The scope of this legal bases should, however, not be understood too narrow. The wording of the GDPR in comparison to Article 6 of the draft ePrivacy Regulation and Recital 13 of the Digital Content Directive shows the GDPR´s intention of including more business models into Article 6(1)(b) GDPR.

´Necessary´ for performing a contract has to be understood which a view on the whole contractual concept. If part of the contract is the supply of a service free of charge (monetising it via advertising f.i.) the provision of such a free service leads to the data processing being necessary for performing such a contract. The freedom to conduct a business includes the guarantee for contractual freedom and the freedom to define and build a business model as long as it operates within the law. Such freedoms are essential for our economy and driving innovation. It is therefore imperative that companies are free to define how they want to offer their services – including the way to monetise their business model. The GDPR itself provides the safeguards necessary to balance the interests of business and users: the risk based approach, compliance with transparency obligations and user rights – to name a few.

In our view, there is no need for the draft Guidelines to restrict Article 6(1)(b) GDPR to situations where it would be altogether impossible to deliver or supply a service without the processing of the specific personal data in question. In Recital 44, the GDPR explicitly states that processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract. This suggest a broader scope and is also supported by general contract law where the contracting parties can shape their contractual relationship as well, can decide which contracts

they want to conclude etc. and are not limited to purposes and measures that are strictly necessary without looking at the context of the contract.

In should also be noted that if the narrow interpretation suggested in the draft Guidelines persists, the contracting parties may end up with contracts that cannot fully be performed since the aim of the contract would require more data processing than what would fall under the definition of the Guidelines.

The Guidelines should furthermore recognize that the question of whether legitimate interests can legitimize a specific processing operation must be answered on a case-by-case basis on the basis of a specific balancing of interests that takes into account the specificities of the processing operation in each case. Consent should not be treated as inherently superior to other legal bases.

According to Recital 47, the reasonable expectations of the data subject based on his relationship with the controller must be taken into account. In addition to the subjective expectations of the data subject, it is also necessary to ask what can be reasonably expected objectively. These expectations cannot be extended by the mandatory information required under the GDPR (Article 13, 14 GDPR).

With regard to the integration of third-party services, it can in any case no longer be assumed that users who have a profile/account with a social media provider or provider of similar services would (subjectively) normally not expect website operators to pass on information to the social media provider. The respective providers usually give extensive information on how their services work and advertisers using their tools. Information is also usually provided on the websites the user visits. The Guidelines obviously also assume this here. Cf. example 6: *[...] She is informed that this data will be collected via social media plug-ins or tracking pixels, the processes are clearly described to her, as well as the fact that targeting involves other entities who are jointly responsible for ensuring compliance with the GDPR. [...]*

Moreover, the opinion should be questioned whether the transfer of data to social media providers really (still) constitutes processing that a data subject should not reasonably expect - especially if the visited website represents a commercial offer with corporate marketing activities, where the inclusion of advertising networks has become standard practice.

We therefore welcome the Board's underlining of the robustness of legitimate interests as a legal basis, recalling that it requires a careful assessment of the risks at hand and must be accompanied by transparency and control. We also agree that, used properly, legitimate interests are a protective, effective way to ground data processing for the purpose of providing personalized content when a serious balancing test shows it is appropriate. At the same time, we would suggest that, in order to clear up the confusion that exists at present, the Board clarify that its position on whether legitimate interests can/does not provide an appropriate legal basis for ad targeting (or ad personalization). Such clarification would support businesses by providing legal certainty.

We are, however, concerned with the suggestion that reliance on legitimate interests (which should only be permissible for the purpose of content personalization) requires "individuals to express a prior objection to its use of social media for targeting purposes". This can be read as tantamount to requiring a form of consent before legitimate interests can be relied on. We would like to underline that GDPR Article 21 is not time bound and does not require a prior right to object when relying on legitimate interests.

Further, paragraph 45 of the guidelines suggests that data subjects should be provided with an opt-out not only when accessing a social media platform, but also be provided with "controls" that ensure the targeting no longer takes place after they have objected. It is unclear how this ´control´ is mandated by Article 21 GDPR and what form of ´control´ the Board is referring to in this instance.

The logical conclusion of the Guidelines suggestions around contractual necessity and legitimate interest is that the EDPB believes there is only one legal basis for the processing of data for personalized ads: consent. Not only is the conclusion at odds with the GDPR — which provides a non-hierarchical list of legal bases — but it also will fundamentally alter the nature of the Internet as we know it, creating poorer experiences for people (who will be flooded with still more consent requests) and adding to the hardships that businesses already are facing.

The Guidelines should recognize that the question whether contractual necessity and legitimate interests are appropriate legal bases should be resolved on a case-by-case basis, using a process that takes into account the specifics of the processing. Consent should not be treated as

inherently superior to the other legal bases, particularly given the burdens it imposes on people to actively manage their data.

The setting or reading of cookies is governed by the requirements of the ePrivacy Directive (2002/58/EC) in the version of the so-called ´Cookie Directive´ (2009/136/EC).

The processing of personal data in connection with the cookies is governed by the provisions of the GDPR. In particular, the possibility of data processing after balancing the interests (Article 6 Para. 1 lit. f GDPR) should therefore be taken into account in this regard. If the weighing of interests is in favour of the website operator, the consent derived from Article 5 para. 3 ePrivacy Directive (for the Federal Republic of Germany, via an interpretation of § 15 para. 3 sentence 1 TMG in conformity with the Directive) need not extend to every data processing.

Against this background, there are many arguments in favour of deleting the following in recitals 71, 72 (with reference to the example of targeting on the basis of observed data):

In addition, any subsequent processing of personal data, including personal data obtained by cookies, social plug-ins or pixels, must also have a legal basis under Article 6 of the GDPR in order to be lawful. ~~For what concerns the legal basis of the processing in Examples 4, 5, and 6, the EDPB considers that legitimate interest cannot act as an appropriate legal basis, as the targeting relies on the monitoring of individuals' behavior across websites and locations using tracking technologies. Therefore, in such circumstances, the appropriate legal basis for any subsequent processing under Article 6 GDPR is also likely to be the consent of the data subject. Indeed, when assessing compliance with Article 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection. Moreover, controllers must take into account the impact on data subjects' rights when identifying the appropriate legal basis in order to respect the principle of fairness.~~

6. Joint Controllership

The Guidelines seem take too broad a view of controllership and joint controllership. The Guidelines would put the legal obligation of becoming a data controller to advertisers for virtually all parts of running an ad campaign — including activities advertisers don't actively control such as reporting insights about ad campaign performance. This broad view of controllership will likely require advertisers to take on new and burdensome compliance obligations. It is particularly striking examples 2 -4). The Board has left little room for controller/processor roles between parties even in circumstances where many ads products and tools are standardised and leave little room for controllers to customize these tools.

E.g. according to the EDPB draft, it should be sufficient for Joint Controllership if the Targeter selects only abstract targeting criteria provided by the Social Network Provider without having any influence on the social network users that will in fact see the ad (Section 5.2.1.).

This goes beyond the principles laid down by the CJEU in the Wirtschaftsakademie and Fashion ID decisions. Assuming Joint Controllership in such cases, in our opinion, clearly overstretches the concept of Joint Controllership.

In such cases, the Provider offers an advertising product on its own responsibility. Solely the Provider is responsible for the classification of its members to certain targeting segments, and data provided by the members for this classification is under a legal relationship between the Provider and its members only. The Targeter has no influence on this and has nothing to do with the personal data that is processed with it; the Targeter does not determine what personal data is to be processed in order to classify the Social Network members.

Placing an advertising order for certain audience segments should not be seen as sufficient for Joint Controllership. The advertising order (by the Targeter) for particular audience segments only sets the occasion for the data processing (by the Provider), but it does not determine its purpose in the sense of Joint Controllership.

Example: If an employee of Company A calls the switchboard of Company B and requests to speak to the corporate data protection officer, then Company A would not ´jointly control´ the processing of personal data by the switchboard operator of Company B (i.e. determining who the requested person is and what their extension number is). Here too, only the occasion for data

processing by Company B under its own control is given by Company A. Even though Company B would not have performed the particular data processing, Company A has not set any purpose, but the purpose was pre-determined by Company B (i.e. switchboard operations); just similar to a Social Network Provider that has pre-determined the purpose for the data processing by operating a segmented advertising service.

As the example shows, setting the occasion for data processing cannot be sufficient to determine the purposes of the data processing. The purpose determined by the Social Network Provider is the provision of a segmented advertising service, and this should be regarded as the sole purpose of the data processing which is not jointly determined by the Targeter.

The Guidelines should take a more balanced view of joint controllership that recognizes that data controllership should map to practical control over how data is used — and only require advertisers to be joint controllers for activities in which they actively participate in and control the data processing.

Where joint controllership does exist, the draft guidelines appear to go beyond the requirements of Article 26 in placing overly prescriptive requirements on joint controllers. For example, paragraphs 87 and 91 go beyond the transparency requirements of Article 26. Paragraphs 124 and 127 are also overly prescriptive: joint controllers are not required by the GDPR to specify the obligations outlined amongst each other. Also, paragraph 126 recommends that joint controllers rely on the same legal basis for processing wherever possible (noting that to do otherwise would cause problems for data subject rights). However, the Board fails to acknowledge that GDPR Article 26 itself overcomes any such difficulties by requiring joint controllers to "determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights" in a transparent manner and to make the essence of this arrangement available to data subjects.

Lastly, paragraph 57 also notes that joint control begins with the collection of the data and continues ´until deletion of the data´. We would suggest deleting this language as this is overly prescriptive and GDPR Article 26 does not mandate that joint controllership exist for the entire lifetime of the data. In practice, a controller might also decide to use the data for another/additional purpose. For example, in the Fashion ID case, the CJEU concluded that a joint controllership existed between the parties *´in respect of the operations involving the collection and*

disclosure by transmission of the personal data of visitors to its website´, but that this joint controllership did not cover any processing before or after that stage. Furthermore, besides the joint purposes, the receiving controller might have additional purposes for the data processing. This should be acceptable provided that there is an appropriate legal basis for it.